A GSM Simulation Platform for Intrusion Detection

Didier Samfat[1], Véronique Devernay, Christian Bonnet

Institut Eurécom - BP 193
06904 Sophia Antipolis- FRANCE
E-mail: {samfat,bonnet}@eurecom.fr

Abstract - **In this paper we present a mobile network simulator which has been developed in accordance to the GSM phase 1 technical specifications. The resulting platform is able to simulate the whole network as well as the mobile stations at the protocol level. The modular approach adopted for the GSM simulator and the functional architecture allow the network model part of program to be easily ported to various applications. The simulator is used in order to test a generic intrusion detection architecture for mobile networks. Other applications based on the layer-3 signalling analysis could easily be implemented with such a platform.**

Keywords: Simulation, protocols, mobile networks, intrusion detection, network architecture, radio interface.

1 Introduction

The advent of mobile networks prompted new network technology requirements and concerns. One of them is the design of an integrated Network Management System (NMS) whose purpose is to provide network service planning, performance monitoring, fault diagnosis and recovery, accounting and security. The complexity of such a NMS is growing in the case of Global System for Mobile (GSM) because in the near future, the goal of GSM is to provide the same service in most European countries: a subscriber will have access to the network managed by different administrative authorities with the same mobile unit. In order to develop a NMS, a mobile network simulator becomes a mandatory requirement as existing networks are not always available for the test of early NMS prototypes during the software development phases. Moreover, even if such networks were available, the provision of a wide range of traffic generators spread over a wide geographic area is costly and difficult to perform. These problems can be overcome by the use of simulators which also present the advantage of exact repeatability of successive runs (useful during software implementation).

In this paper, we describe the GSM simulation model allowing a mobile user to view the system as a real implementation of the network. Then, we present an application of the resulting platform consisting in testing a dedicated NMS whose main purpose is to provide intrusion detection services.

2 GSM Architecture Overview

In the GSM architecture the whole network is referred as the Public Land Mobile Network (PLMN) which is composed of three parts with reference to Figure 1: the Mobile Station (MS), the Base Station Sub-system (BSS) and the Network Switching Sub-system (NSS). The MS has two components: the Mobile Equipment (ME) (the hardware equipment available from a dealer) and the Subscriber Identity Module (SIM) which is a smart card containing the subscriber's data. This allows the application of one of the principles of Personal Communications, as a call is not directed to a particular piece of hardware but to a subscriber who personalizes an MS by inserting his SIM into the ME.

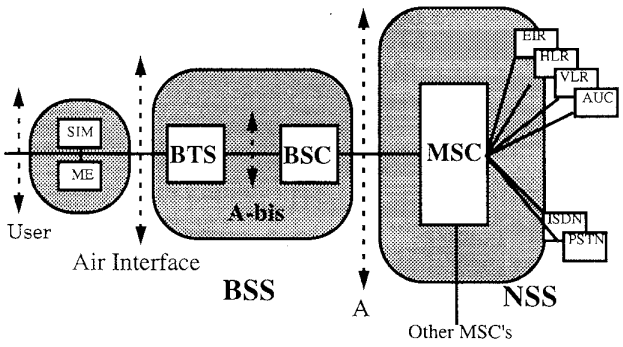

Figure 1: GSM System Architecture

The BSS is in charge of providing and managing transmission paths between the MS and the fixed network; it is composed of the following functional blocks:

- **Base Transceiver Station** (BTS). The BTS is the radio part of the fixed network, communicating with the mobile stations through the air interface and also performing measurements of the quality of the radio communications.

1. The work of D. Samfat on intrusion detection was part of a joint project funded by IBM Zürich Research Laboratory

0-7803-2486-2/95 $4.00 © 1995 IEEE

- **Base Station Controller** (BSC). The BSC is in charge of radio resources allocation; it relays messages concerning call control and mobility management between the MSC and the MS, and also takes handover decisions according to measurement results.

The NSS performs switching functions and communications management functions in order to connect the MS to the desired networks or to other MSs: it is composed of the following entities:

- **Home Location Register** (HLR). The HLR is the main database of the system. It stores informations about the subscribers such as subscription type and current location.
- **Mobile Switching Centre** (MSC). The MSC is the switching centre of the network managing the call control and the mobility aspects. It communicates with the HLR for the location updating procedures, with other MSCs for handover[1], and with the Gateway MSC for the routing of incoming calls. The Visitor Location Register (VLR) is a local database holding some of the information contained in the HLR concerning the MSs managed by the current MSC.
- **Gateway MSC** (GMSC). The GMSC is a gateway for incoming calls providing access to other PLMNs. When a call is directed to a subscriber of the PLMN, it questions the HLR about the current location of the MS and forwards the call to the respective MSC.

3 The Network Simulator

The GSM network simulator has been developed with OPNET software [11]. The resulting platform model simulates the BSS, the NSS and the MS as described in section 2. All layer-3 messages exchanged by the different GSM entities have been implemented in accordance with the GSM phase 1 recommendation.

3.1 Design Criteria

In addition to the basic requirement of designing a GSM simulator as close as possible to the real network, the following design criteria have been taken into account:

- **Portability**: Since the simulator has been programmed in C language it can run on different hardware/software architectures.
- **Scalability**: The platform is able to simulate a GSM network composed of several PLMNs. This requirement is important if we want to predict the behaviour of interconnected PLMN.
- **Customizability**: Various GSM network topologies can be created. For instance, a location area can be composed of one to several cells.
- **Flexibility**: Specific variables of the different entities and functions of the GSM simulator are easily parametrizable.

3.2 The Platform Node Model

All GSM entities of the NSS and the BSS are OPNET network nodes; each network node is composed of one or several processors [2] and of several emitter-receiver pairs for the network connection. The main function of these processors is to manage the different GSM protocols (RIL-3, MAP, BSSMAP) [9], [10]. In addition to the GSM entities, a special node representing the PSTN (Public Switching Telephony Network) has been defined in order to simulate mobile originating and terminating calls. In the platform, the VLR is integrated to the MSC node[3].

The MS is a more complex node in contrast to the other GSM entities. At the network node level, various parameters such as trajectory, speed, altitude of the antenna for the radio-propagation can be set at simulation time. Moreover, the MS requires the coordination of 9 different processors: the subscriber, the SIM card, the man-machine interface, 4 protocol layers (Radio Resource, Mobility Management, Call Control and Physical Layer) [6, 9], the measurements computation, and of the radio equipment. Additional parameters such as call frequency and call duration, allow the definition of the mobile user behaviour.

3.3 The Process Model of the Processors

Each processor is associated to a finite state machine (FSM); each state in the FSM corresponds to a special function. For instance, the MS is able to handle up to 7 different cells simultaneously and 9 FSMs are needed to insure the inter-operability of the 9 processors of the MS. The FSM representing the mobile user has been programmed in order to start or to end a call at any time. Hence, during a call the MS measures the quality of the reception and sends the results to the network. Upon

1. Changing of cell without interrupting the call

2. Depending on the complexity of the GSM component
3. As it is usually done in real GSM networks

receiving the results from the MS, the BSC is able to decide wether or not to perform a handover and to choose the best cell for the MS. Moreover, additional FSMs have been implemented in order to perform all GSM protocols allowing the location update and the handover [7, 8]. However, in order to reduce the simulation time and to test the platform for the intrusion detection architecture, all communications are assumed to be reliable[1].

3.4 Implemented Procedures

The simulator is able to perform the following procedures specific to digital cellular mobile networks:

Location updating (locup). This procedure is triggered by the MS each time its current location area changes. The corresponding information is sent by the BTSs on their control channel. The goal of this procedure is two fold: first, it allows the HLR to know which MSC is currently in charge of the MS, second, to register the MS in the VLR of the current MSC. The location updating request emitted by the MS is processed by the new MSC: if the old location area was already under its control, an ***inter-BSC-locup*** procedure is performed and the MSC has only to update the VLR. However, if the old and new location area are under the control of distinct MSCs, an ***inter-MSC-locup*** is performed. Then, the old MSC informs the HLR of the MS registration in the new VLR, as well as its de-registration in the old VLR.

Mobile Originating call (MO). The mobile user can make a call towards the PSTN; the frequency and duration of these calls are parametrizable. The MSC relays the call request to the PSTN and establishes the connection [2].

Mobile Terminating call (MT). Calls can also be initiated by the PSTN which asks the Gateway MSC for routing information. Therefore, the GMSC asks the HLR for the roaming number provided by the current VLR and routes the call toward the current MSC. The MS is then paged in the location area where it was previously registered. Upon an answer of the MS, the MSC establishes the connection.

Handover. During a call the BSC continuously analyses the measurements results sent by the BTS in order to decide on a potential handover . The following procedures are performed depending on the type of handover:

- ***internal-handover***: the MS is moving from a current cell to a target both managed by the same BSC
- ***inter-BSC-handover:*** the MS is moving to a target cell managed by another BSC in the same MSC area
- ***inter-MSC-handover:*** the MS is moving from the anchor MSC [3] area toward a target cell of another MSC area (relay MSC area)
- ***subsequent-handover***: the MS moves from the relay MSC area to another relay MSC area, or is back to the anchor MSC area

4 IDAMN: Intrusion Detection Architecture for Mobile Networks

The GSM platform has been implemented in order to test a NMS which provides only intrusion detection services. The reasons for such a choice are twofold. Firstly, the GSM network does not provide intrusion detection services to operators. Secondly, configuration, accounting and fault management functions are present in various management environments in contrast to performance and security management functions which are more difficult to implement as they require data collection and thus create computational overhead. Therefore, the challenge was to model IDAMN in order to detect an intruder «***on-line***» while minimizing the overhead incurred at the GSM network.

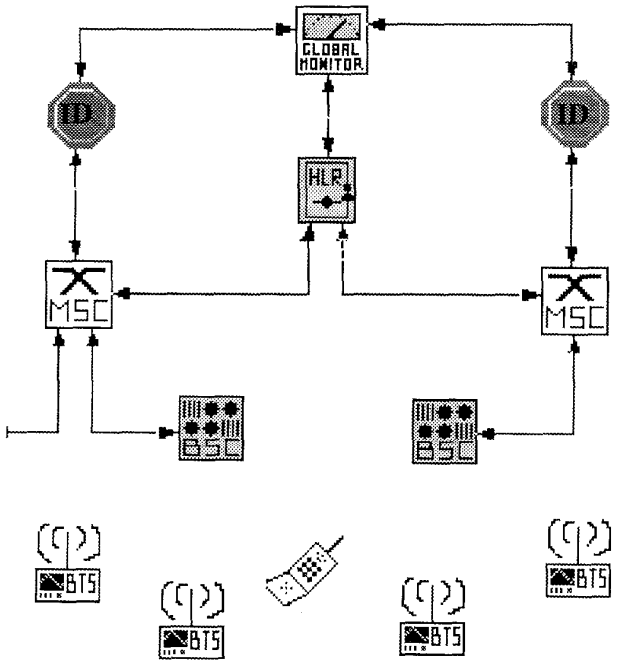

Figure 2: A Portion of the Global Architecture developed with OPNET.

1. The loss of messages is not yet simulated
2. Speech data traffic is not yet simulated
3. MSC managing the MS at the beginning of the call

4.1 Multi-Level Intrusion Detection

The basic idea of detecting an intruder relies on the system ability to learn the normal behaviour of the subscriber by creating a ***profile***. An intruder impersonating the real subscriber will have a different behaviour and thus will generate a significant deviation from the standard profile [2, 3, 4]. Therefore, forbidding a mobile user to lend his MS becomes a mandatory security policy. The following three levels of analysis have been defined:

- ***Level 1:*** The resulting procedures allow a fast intrusion detection analysis by verifying the speed of a mobile user or existing clones (the same user being active in two different parts of the PLMN at the same time).
- ***Level 2:*** The system measures the impact of the subscriber behaviour on the different GSM entities (an abnormal activity of a MSC may be a symptom of intrusion).
- ***Level 3:*** This is the most significant intrusion detection analysis as the resulting procedure evaluates every deviation from the normal user's «signature» (normal behaviour profile).

In the case of the level-3 analysis the normal behaviour of the subscriber is defined by three profiles: mobility-profile, activity-profile and speech-profile. Each profile will help in raising different intrusion alarms that a ruled based system will analyse in order to give the final diagnostics.

4.2 IDAMN Entities

The relevant pieces of information for modelling the user behaviour as well as to detect an intrusion are distributed over different entities of the GSM architecture. In order to minimize the computational overhead incurred at both IDAMN and GSM, the procedures addressing the different level of intrusion are spread over two dedicated machines: the Global Monitor and the Intrusion Detector.

The Global Monitor (GM). The main purpose of the GM is to create and update the subscriber normal behaviour profile upon receiving new audit data from the intrusion detector. The profile updating procedure is performed off-line during peak-off hours. The GM is able to send the profiles on request of the intrusion detector as well as to perform level 1 and level 2 of intrusion detection (the GM is the only entity of the network which is able to detect a clone appearing in a different MSC area). The results of these two preliminary analyses are processed by a rule based system which generates a *global report.*

The Intrusion Detector (ID). The ID functional architecture is depicted in Figure 3. The ID performs level 1 (detection of a clone at the location area level) and level 3 of intrusion detection. Upon receiving new audit data from the anchor MSC, the ID requests the GM the different behaviour profiles as well as the global report concerning the mobile user. Then, the ID is able to decide if there is a potential intrusion.

4.3 Interfacing IDAMN and GSM

The global architecture is depicted in Figure 2, the IDAMN components have also been programmed with OPNET. The GM is able to access the HLR via the GSM standard protocol MAP/C in contrast to the ID which can retrieve information from the VLR using the MAP/B protocol [10]. Moreover, a single ID is associated with each MSC; as the anchor MSC is the only entity to have a complete view on the mobile user activity and mobility, it sends to the ID additional useful data unavailable in the VLR.

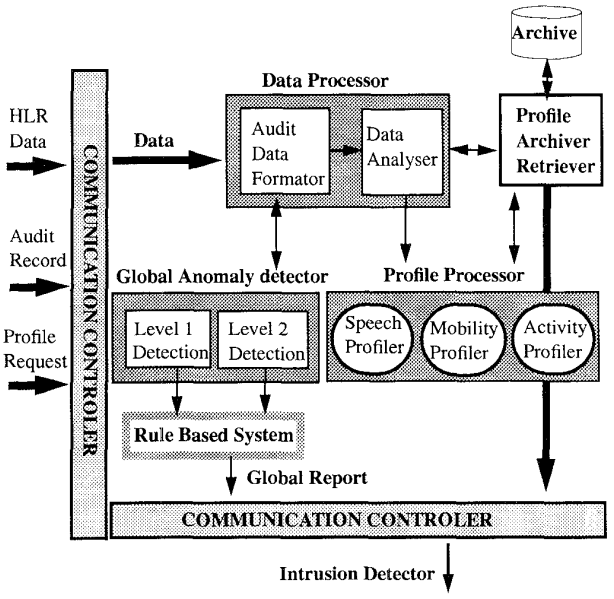

Figure 3: The Global Monitor Functional Architecture

The verification of the speaker has not been implemented yet. However, we have some promising results in monitoring the activity and mobility behaviours. The relevant measures for the current version of IDAMN are the activity and mobility measures.

Activity Measure. This measure is made over several parameters related to the MO/MT calls. A statistical behaviour profile is computed over the following parameters: time and duration of a MO/MT call, number of handovers performed, time and duration of activation of the MS, frequency of outgoing and incoming calls. The values of these parameters are obtained when the anchor MSC performs the following procedures: *mo-call-start/*

stop, mt-call-start/stop, imsi-attach/detach, internal-handover, inter-BSC-handover, inter-MSC-handover and *subsequent-handover.*

Mobility Measure. This measure allows us to analyse the mobility area of a subscriber as well as the most frequent paths used. A mobility behaviour profile based on a Markov model is established depending on the location areas the mobile user used to cross. This mobility profile is updated when the following procedures are performed: *inter-MSC-locup, inter-BSC-locup.*

Intrusions alarms are raised when the detector notices a strong deviation of the mobile user behaviour compared to the mobility and activity profiles. Next, these alarms are analysed by a rule based system which gives the final diagnostics.

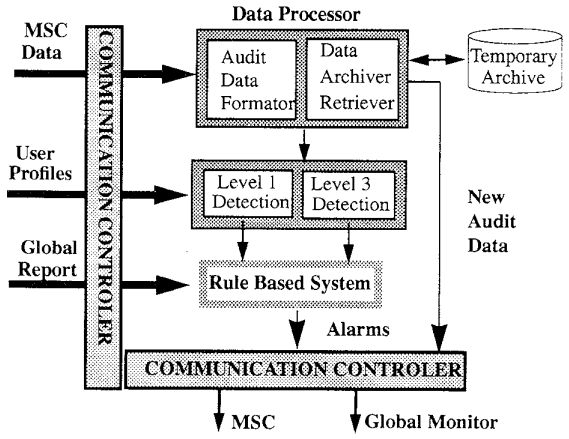

Figure 4: The Intrusion Detector Functional Architecture

5 Conclusion

This paper presented a GSM simulator which was used to test a NMS dedicated to intrusion detection. The GSM simulator was designed in a modular form in order to fulfill portability, scalability, customizability and flexibility requirements. The Intrusion Detection Architecture for Mobile minimizes the computational resources incurred at the GSM network. Preliminary testings of the components of IDAMN are promising as we are able to have a complete overview of the mobile úser behaviour which increases our ability to detect an intrusion.

References

[1] M. Mouly, M.B. Pautet, *The GSM System for Mobile Communications*, **ISBN 2-9507190-0-7,** 1993

[2] T.F. Lunt, *IDES: An Intelligent System for Detecting Intruders*, **Proc., Symposium on Computer security, Threat and Countermeasures,** Roma, Nov1990

[3] K. Ilgun, P.A Poras, R.A Kemmerer, *USTAT a Real-Time Intrusion Detection System For Unix*, **SRI Intrusion Detection Workshop**, Paolo Alto, CA Feb. 1989

[4] S.E. Smaha, *Haystack: An Intrusion Detection System*, Proc., **IEEE Fourth Aerospace Computer Security Applications Conference**, Orlando, FL, Dec. 1988

[5] B. Mukherjee, L.T. Herbelein, K.N. Levitt, *Network Intrusion Detection*, **IEEE Network Magazine**, May/June 1994, VOL. 8 No 3.

[6] GSM Recommendation 3.05, *Signalling Requirements Relating to Routing of calls to Mobile Subscribers*, **ETSI Standard**, Feb. 1992

[7] GSM Recommendation 3.09, *Handover Procedures*, **ETSI Standard**, Feb. 1992

[8] GSM Recommendation 3.12, *Location Registration Procedures*, **ETSI Standard**, Feb. 1992

[9] GSM Recommendation 4.08, *Mobile Radio Interface Layer-3 Specification*, **ETSI Standard**, Feb. 1992

[10] GSM Recommendation 9.02, *MAP Specification*, **ETSI Standard**, Feb. 1992

[11] *OPNET Network Simulation Software*, MIL 3, Inc. 3400 International Drive, Washigton, DC 20008, **Release 2.4.A**